ASSESS YOUR VULNERABILITIES

Maintain a continuous understanding of assets and manage vulnerabilities in real time
Integrate data and processes to make vulnerability management more effective and efficient

The Situation
Understanding and effectively managing system vulnerabilities are fundamental and critical steps in any security management program. For example, the first four Critical Controls for Effective Cyber Defense (formerly the SANS Top 20 Security Controls) involve identification and inventory of devices and software, hardening of configurations, and regular and automated system vulnerability assessment and mitigation. These controls also represent much of the first phase of the US Department of Homeland Security’s Continuous Diagnostics and Mitigation (CDM) Program.

Industry experts recommend investment in these areas because the accelerating rate of change in IT environments, combined with an expanding threat landscape, has led to an increase in system vulnerabilities. Without complete and ongoing visibility into your organization’s critical IT systems, applications, and information, along with accompanying vulnerabilities, the probability of exploits and compromise rises dramatically.

One of the problems is that most organizations treat vulnerability management as an occasional and isolated exercise, largely focused on addressing immediate compliance requirements. They often overlook the dynamic nature of assets and threats. And they fail to continuously discover and leverage information about hosts, vulnerabilities, and prospective controls that could help them facilitate mitigation and remediation.

For example, information technology vendors are constantly discovering and announcing their products’ vulnerabilities and releasing the remedial patches. New assets often appear on the network faster than they can be discovered and catalogued. Mobile devices are constantly coming and going. A vulnerability management system that isn’t solidly interconnected with an asset management system and a closed-loop analytics and remediation process is doomed to remain an ongoing, inefficient set of fire drills.

Driving Concerns
Most organizations have a vulnerability assessment (VA) tool of one sort or another, and often more than one. These basic tools are effective at the specific task of cataloguing vulnerabilities that exist on hosts, but tend to be disconnected, deployed primarily to meet compliance mandates that dictate the need. The valuable data they glean about hosts remains siloed, detached from security management analytics and processes that could provide crucial context. This hurdle must be overcome, since the data from a well-managed vulnerability management program is exactly the cornerstone input needed to support an optimized security and compliance program.

Vulnerability assessment solutions tend to remain in this standalone, tactical state for a number of reasons:

- **Lack of connectivity with a comprehensive source of asset information.** Before you can assess a device, you must first know it exists, and then determine what it is and its location. While many tools provide for rudimentary asset discovery, this basic information can’t offer the essential context needed for real-time asset inventory, device profiling, user identification, physical network topology creation, virtual environment mappings, and remediation workflow integration.
Assessing Vulnerabilities

Decision Elements
These factors could influence your architecture:

- What types of VA reports will you require? How often will you need to generate them? Are there different organizations that require specific reports related to their responsibilities?
- How does your current vulnerability remediation process work? Who requires the information detailing the specific vulnerabilities that need to be addressed? What’s the most efficient way to provide that information? Is there an existing ticketing system?
- Do you use McAfee® ePolicy Orchestrator® (McAfee ePO™) software today to manage endpoint security or other technologies?
- What regulatory requirements apply to your business that might affect your VA solution architecture?

- Good view of the network, poor view of the enterprise organization. An effective solution needs to know not only where the active assets are on your network, but should also be able to link them to their roles in your business. For example, vulnerability assessment and reporting are very different for a point-of-sale kiosk compared with an executive laptop, e-commerce server, or transient BYOD devices.
- Multiple tools to do one job. Many organizations do a reasonably good job of identifying straightforward vulnerabilities on known servers and workstations. But assessing specific web applications, databases, and a variety of mobile devices often proves to be extremely challenging. Use of a disjointed set of VA tools only exacerbates the problem, since incorporating each of these special-purpose VA tools into your enterprise infrastructure adds complexity and cost.
- Poor remediation workflow. The focus of many vulnerability assessment programs is gathering data and generating reports. This is only the beginning. A truly effective program categorizes and prioritizes vulnerabilities, taking into account severity of the vulnerability and the relative value of each vulnerable asset. Next, it is critical to get this information directly into the hands of the people who need to take action.
- Inability to translate vulnerability into risk. Most organizations today have far more vulnerabilities in their network than they are able to address with their available staff. However, not all vulnerabilities are created equal. Many vulnerabilities are mitigated by countermeasures or other security controls, are on assets that are low value, or are highly unlikely to be exploited for other reasons. A good VA program and its tools should provide the guidance you need to fix what’s most important first.

Until these fundamental challenges are addressed, it’s difficult for organizations to leverage the information they have gathered to transform raw data into actionable intelligence. As a result, they tend to spend a great many resources on discrete VAs, often with little measurable improvement in risk posture.

Solution Description
To achieve efficient vulnerability assessment, it is necessary to step beyond point products and disparate tools and integrate vulnerability assessment into a broader enterprise workflow. An ideal solution combines the following capabilities into a cohesive framework:

- Comprehensive asset discovery. Asset discovery can be performed both actively (via scanning) and passively (via network listeners). Regardless of the technique, all assets should flow into a common repository for management and data collection should be in real time.
- Asset management. Asset management ensures that each scanned asset and its inventory data are properly sorted and categorized to support efficient scanning, reporting, and remediation. Assets may need to be organized by geography, business unit, application, compliance, or combinations of these attributes. Assets also may require criticality or value to be assigned by administrators, so that remediation can be prioritized. Finally, assets should have owners associated with them, so that the proper personnel can be assigned for remediation.
- Comprehensive vulnerability scanning. Vulnerability scanning should provide the ability to deeply assess in real time a wide variety of platforms, including Microsoft Windows, UNIX, Mac OS, mobile devices, virtual environments, storage, and network infrastructure. In addition to looking at operating systems, administrators should also have the ability to assess web applications and databases, eliminating the need for multiple tools that accomplish essentially the same thing.
- Flexible reporting and remediation workflow. Many VA implementations begin with simple reports that business owners use to demonstrate compliance with relevant regulatory requirements. They highlight broad areas that require remediation. At a minimum, the VA solution needs the flexibility to produce the reports dictated by the business. As your vulnerability and risk management processes mature, however, you will require a more open framework to support deeper, automated analysis of the risk associated with vulnerabilities, ensuring that the right individuals are fixing the right things in the right order.
Technologies Used in the McAfee Solution
The McAfee® solution has several components designed to work together as a cohesive solution.

- **Real-time asset discovery.** McAfee Vulnerability Manager with the included McAfee Asset Manager module offers real-time active scanning as well as passive network discovery and monitoring. McAfee Vulnerability Manager can detect anything with an IP address, identifying all networked assets, even assets located in air-gapped and critical infrastructure environments. In addition, McAfee Asset Manager passively monitors network traffic in real time to discover and map everything on your network, capturing transitory, virtual, and mobile devices. While it watches for and reports on new devices, it enumerates devices, patterns, and communications—details that help you gauge and mitigate risk. It tracks devices based on a media access control (MAC) address, preventing inaccurate device information if a device IP address changes.

- **Unified asset management.** McAfee Vulnerability Manager integrates directly with enterprise asset management tools, including LDAP, Microsoft Active Directory, and the McAfee ePO management platform, so that you can maintain one central repository for asset data. Assets can be grouped, assigned owners, and given their own “personalities” based on their business function and asset criticality. If you are using McAfee ePO as your authoritative asset inventory, data collected by McAfee Vulnerability Manager/McAfee Asset Manager flows directly into the McAfee ePO database. The asset profile you create can include hardware, software, user, and network attributes. Once in the McAfee ePO environment, McAfee ePO’s tagging and system tree functions and integration with Active Directory help you group and categorize assets, reflecting attributes such as business unit, chassis type, user, system function (such as Microsoft Exchange Server vs. laptop), and location (network and geographical).

- **Comprehensive vulnerability scanning.** In addition to identifying open ports and configurations, McAfee Vulnerability Manager makes system and application-level assessments that include database banners, policy settings, registry keys, file and drive permissions, and running services. The product tests more than 450 operating system versions to detect the broadest range of vulnerabilities. You can augment predefined checks and updates for zero-day threats by writing custom scripts and checks to test proprietary and legacy programs. McAfee Vulnerability Manager also assesses third-party content that follows XCCDF, OVAL, and other SCAP standards and can catch malicious content, including Trojans, viruses, and other malware. The McAfee Web Application Assessment Module is sold separately and extends scanning coverage to reveal web application vulnerabilities and coding mistakes. In addition, McAfee Vulnerability Manager for Databases can give you complete visibility into your overall database security posture, providing you with a detailed risk assessment across more than 4,700 vulnerability checks.

- **Flexible reporting and remediation.** These McAfee systems work together to provide automated monitoring and management of scanning, remediation, enforcement, and reporting. This integration helps you avoid time-consuming fire drills and ad hoc processes, eliminate errors, and protect more systems more efficiently. To keep your risk assessment up to date, McAfee Vulnerability Manager and McAfee Risk Advisor can pull in threat feeds from McAfee Labs to give insight into dynamic threats as well as remediation guidance. McAfee Risk Advisor works with McAfee Vulnerability Manager to create a unified environment for understanding evolving risk and making risk-based decisions based on existing countermeasures, relevant risk, and asset value, in keeping with the latest best practices recommended by government and industry experts.
The McAfee solution provides comprehensive, risk-based vulnerability assessment over the network, unified by McAfee ePO software.

**McAfee Vulnerability Manager**

The core of the McAfee vulnerability assessment solution, this system performs several key tasks. In the simplest model, McAfee Vulnerability Manager is a highly scalable standalone solution for host discovery, asset management, vulnerability assessment, and reporting on any network-connected device. As your needs expand, McAfee Vulnerability Manager integrates cleanly with the other components in the McAfee solution, including the web application and database modules, to protect and leverage your investments and help you improve your risk management practices.

**McAfee Vulnerability Manager: Asset Manager Module**

This feature of McAfee Vulnerability Manager increases asset and network visibility through always-on passive discovery and monitoring. As it monitors traffic, the system will discover and map everything on your network, including rogue devices, forgotten VMware hosts, and mobile devices. Device details are automatically sent to McAfee Vulnerability Manager for immediate assessment and can leverage
dynamic system tagging for full automation. In addition, McAfee Asset Manager can perform a full software and hardware inventory on each asset it discovers, storing this information in the McAfee ePolicy Orchestrator database to create an authoritative asset repository.

**McAfee Vulnerability Manager: Web Application Assessment Module**

Deep web application scanning can help you uncover and address common coding mistakes and vulnerabilities as part of a vulnerability management lifecycle. What makes it unique is that it treats web applications as business assets, just like a server, router, or other high-value assets. This is important since web applications have business value and therefore have asset owners and varying levels of criticality.

The Web Application Assessment Module covers commonly exploited web application vulnerabilities and weaknesses in the market today. Specifically, the Web Application Assessment Module includes the required checks for PCI DSS, as well as coverage of the OWASP Top 10 and the CWE-25 categories. All workflow and reporting is seamlessly integrated with native McAfee Vulnerability Manager capabilities and may be performed via McAfee ePO software as well.

**McAfee Vulnerability Manager for Databases**

Use this solution to evaluate risk for leading database systems such as Oracle, Microsoft SQL Server, IBM DB2, MySQL, and others. It can reveal missing database patches, unsecured database accounts, high-risk code, and other classes of vulnerabilities. McAfee Vulnerability Manager for Databases is a simple extension to McAfee ePO software and leverages native functionality for reporting and workflow.

**McAfee ePO software**

This policy management framework serves as a central repository for asset management and reporting across the combined vulnerability assessment solution. McAfee ePO software collects information about assets via multiple discovery techniques, including active and passive scanning from McAfee Vulnerability Manager, or passive sensing via McAfee ePO software rogue system detection. Discovered assets are then grouped, tagged, and managed via McAfee ePO software for use in scanning tasks and reporting. McAfee ePO software also collects and collates vulnerability information from all parts of the McAfee solution, providing centralized dashboards, reporting, and automated workflow for dealing with vulnerability remediation.

**McAfee Risk Advisor**

McAfee Risk Advisor is an analytics engine that brings in:

- Threat feeds from McAfee Labs.
- Asset inventory and mapping details from McAfee Asset Manager.
- Vulnerability information from McAfee Vulnerability Manager.
- Associated remediation information from McAfee ePO software, including criticality, specific security controls (countermeasures) that are deployed in your environment, and how they are configured.

By combining detailed information about host security posture with up-to-date information about emerging threats, McAfee Risk Advisor highlights exactly which vulnerabilities are most critical, correlated with the most valuable assets, helping you prioritize and address the most pressing issues.
Optional Integrations

**McAfee Network Security Platform**
This network intrusion prevention system (IPS) can import vulnerability details from McAfee Vulnerability Manager, providing crucial security posture details to the IPS analyst. Correlating attacks with host vulnerabilities improves the relevancy of the alerts generated by McAfee Network Security Platform and allows IPS analysts to more quickly identify the most critical security events.

**McAfee Enterprise Security Manager (SIEM)**
The McAfee security and information event management (SIEM) system can give you a single environment to consolidate, correlate, and report on security events and data from hundreds of data sources, including the McAfee products in this solution. It can enrich the vulnerability assessment process with contextual information from identity, authentication management system, compliance and other systems to give you a more complete understanding of how network and security events correlate to business processes and policies. It also facilitates audit and compliance activities for hundreds of regulations.

**Real Time for McAfee ePO**
An add-on option for McAfee ePO available with McAfee endpoint suites, this software can collect host information instantly and efficiently across the network. You can gather up-to-date details about McAfee software on specific systems or groups of systems and ensure that defenses are installed, active, up to date, and enforcing the right policies. Best practice queries and an optimized design show you security status for managed clients in moments. Administrators see details in context and can remediate security issues as events are happening, not after the fact. In large or complex environments, the design delivers this knowledge up to a thousand times faster than with standard McAfee ePO software.

**Impact of the Solution**
Deploying the McAfee solution addresses the driving concerns outlined at the beginning of this document.

- Connects vulnerability assessment and real-time continuous monitoring to a comprehensive source of asset information, providing the context needed for relevant asset inventory, reporting, and workflow.
- Allows for real-time discovery of devices immediately upon connection, providing visibility into both the network and the enterprise organization, telling you where the active IP addresses are on your network and their roles in your business.
- Consolidates a tool for host vulnerability assessment with tools for assessing web applications and databases to improve risk management while reducing complexity and cost.
- Helps correlate vulnerabilities with associated risk to assist with prioritization of affiliated mitigation activities.
- Improves remediation workflow, facilitating fast and efficacious corrective actions.

McAfee reduces the cost of integrating vulnerability assessment with other enterprise processes, such as compliance reporting and patch management, to help you manage these increasing vulnerabilities with the fewest possible resources and fulfill the core elements of a continuous diagnostics and mitigation program.
Additional Resources
www.mcafee.com/vm
www.mcafee.com/vmfordatabases
www.mcafee.com/riskadvisor
www.mcafee.com/epo
www.mcafee.com/producttrials

For more information about the Security Connected Reference Architecture, visit:
www.mcafee.com/securityconnected.